EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
Informatics Security

Brussels, 21/06/2011
HR.DS5/GV/ac ARES (2011) 663475
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON CONTROLS AGAINST MALICIOUS CODE

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 21/06/2011

Version 18/03/2011

TABLE OF CONTENTS

1. ADOPTION PROCEDURE

This Security Standard is adopted in accordance with Article 10(3) of Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission, adopted on 16 August 2006.

It is drawn up under the responsibility of the Security Directorate pursuant to Article 9(1)(b) and takes into account the items listed in Article 10(2) of Commission Decision C(2006)3602, in particular internationally recognised norms and standards applicable in the field of information systems security.

Under Article 10(3) of Commission Decision C(2006) 3602, the implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature proposed by the Director of the Security Directorate and adopted by the Director-General of the Directorate-General for Human Resources and Security in consultation with departments that have a legitimate interest. These supplementary measures are called 'security standards' where their application is mandatory, or 'security guidelines' where their application is optional or where they provide guidance on security standards implementation

2. INTRODUCTION

Malicious code can be defined as "software which interferes with normal operation of a computer system". Another definition might be "software which executes without the express consent of the user". Malicious code is therefore a threat for the integrity, availability and confidentiality of data.

The main concern of this standard is to implement effective and efficient prevention, detection and correction against malicious code and related security incidents.

3. SCOPE

The scope of this document is limited to protection of information systems against malicious code by means of dedicated software often referred to as "anti-virus software" (also "anti-malware" or "virus protection software").

Issues such as "spam" or mobile code which share common patterns with malicious code have not been considered in this document. These issues will be treated in separate standards.

Other preventive measures that can help to protect against malicious code, such as intrusion detection/prevention systems, patch management, network authentication or firewalls, are also not covered in this standard.

Aspects of incident management and patching of system vulnerabilities relevant for malicious code protection are briefly addressed in this document. For further

information it is advised to consult the Standard on Information Systems Security Incident Management

4. TERMINOLOGY

The colourful names given to different types of malicious code reflect different approaches to malicious programming: for example virus, Trojan horse, worm, logic bomb, spyware and adware. Some of them are explained below.

The term **computer** used in this standard refers to all machines, including servers, gateways, NAS, mail gateways and workstations, including laptop computers, notebooks and handheld computing devices (e.g. PDAs).

Malware: short for "malicious software"; malware is another name for malicious code and refers to software programs designed to damage, spy or perform other unauthorised actions on a computer system such as viruses, Trojan horses, worms, logic bombs, etc.

Virus: A program that attaches itself to an executable file or application and delivers a payload that ranges from being just annoying to extremely destructive to computer's hard drive, files and programs in memory, and that can replicate itself to other disks. A file virus executes when an infected file is accessed. Also a generic term for any type of malware, and used as such hereafter.

Trojan horse: A Trojan horse, or Trojan for short, is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorised action like unauthorised access to the user's computer system.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. Some worms are security threats, using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it needs not to be attached to particular files or sectors at all.

Spyware: A computer software that is installed surreptitiously on a personal computer to collect information about a user or his/her computer or data without the user's informed consent.

Adware: Software which displays advertisements, whether or not the user has consented. Adware will often also be spyware that displays advertisements related to what it finds from spying user's data.

Keylogger: Software programs which logs the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their input is being monitored and the captured data used for malicious purposes.

5. SECURITY CONTROLS

Policy objective 5.4.1: Permanent controls must be applied to prevent and detect the introduction of malicious software. Detection and prevention measures and appropriate user awareness procedures must be implemented.

5.1. Risks targeted

Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms and Trojan horses. Security controls defined in this security standard cover the following threats: computer viruses, network worms and Trojans, etc. These security controls do not protect against threats originating from interpreted language applications (e.g. Java), cross-site scripting, etc[1].

Non-compliance with this standard will result in greater risk of information systems being infected by malicious code that can:

(1) Result in the loss of information/data and software on European Commission systems.

(2) Increase the cost of computing maintenance and cause network downtime by malicious code outbreaks that will divert processing power and human resources to the task of watching out for and cleaning up after malicious code infections, attacks or outbreaks.

(3) Result in loss of reliability of systems threatened by malicious code that spread from system to system across networks, and that can cause disclosure of European Commission sensitive data or worms that clog memory and storage facilities and slow down the systems.

(4) Result in loss of reputation for the European Commission.

Related threats from the "Standards on Risk Management (Appendix B)"

Threat identification	**Impacted security needs**
T23 – Disclosure	Confidentiality
T26 – Tampering with software	Confidentiality, Integrity, Availability
T36 – Corruption of data	Confidentiality, Integrity

[1] For these, see the Standard on Mobile Code.

5.2. Security Controls statements

Typical controls to protect against malicious code use technology, policies, procedures and training, all applied in a multi-layered[2] manner from perimeters inward to hosts and data. The controls are of the preventive and detective/corrective variety. Controls must be applied at the hosts, servers and networks.

5.2.1. Configuration

Virus[3] protection software must be configured to:

(a) scan computer memory, executable[4] files (including macros contained in data files), data files including protected files (e.g. compressed or password protected files,), and removable storage media; all files not scanned for any reason must be logged in the antivirus history logs;

(b) scan and filter incoming and outgoing traffic (including e-mail and downloads from external networks such as the Internet);

(c) be active at all times (on-access scanning);

(d) provide an alert when a suspected virus is identified;

(e) comply with a standard reference configuration[5] for the anti-virus software[6];

(f) disinfect, delete, rename or quarantine viruses when identified;

(g) ensure that end users cannot disable virus protection features or minimise core functionality;

(h) update virus recognition files used by virus protection software, virus protection software engines, patches, virus protection software versions, whenever new ones are released;

---

2 Layered defence: a combination of security services, software and hardware, infrastructures, and processes which are implemented to achieve a required level of protection. These mechanisms are additive in nature with the minimum protection being provided by the network and infrastructure layers. Layer has to be understood in this context in the document.

3 "VIRUS" is used with the meaning of "VIRUS", "SPYWARE", and "ROOTKIT", etc…

4 Not only *.EXE but all the files that could be executed by the operating system (e.g exe, bat, pif, scr, etc.)

5 A configuration that has been tested and qualified internally before becoming a standard configuration to be installed on all information systems.

6 "ANTI-VIRUS SOFTWARE" is used with the meaning of "ANTI-VIRUS", "ANTI-SPYWARE", and "ANTI-ROOTKIT SOFTWARE".

(i) have multiple trusted updating sources and mechanisms, internal and external sources (failover mechanisms);

(j) ensure that virus protection updates are distributed to all servers/computers automatically and within a critical timescale, prioritised by their importance;

(k) log all alerts regarding the antivirus activity and send them to a central antivirus server (alerts should be monitored);

(l) regularly run a full scan on all computers to minimise the risk of having virus(es) not yet detected because they were already residing in these computers before the application of the antivirus updates that allow their detection via on-access scanning;

(m) regularly send reports about the antivirus to the relevant personnel (see section 5.3 Roles and Responsibilities).

5.2.2. Installation and procedures

To reduce the risk of virus infection the following controls must be applied:

(a) evaluating virus protection software prior to purchase;

(b) installing virus protection software on all computers, e.g. servers, gateways, NAS, mail gateways, and workstations, including laptop computers, notebooks and handheld computing devices (e.g. PDAs);

(c) traffic which passes through different layers, computers or systems across the information processing environment must be scanned by at least two different software products (e.g. an email message coming in would be scanned by two different products, one on the network periphery layer and the other on the email server; files downloaded from internet would be scanned at the proxy level as well as on the client layer - workstation or server).

(d) implementing emergency procedures for dealing with virus incidents, so that the virus spread is stopped and adequate measures are applied;

(e) procedures for sending "virus" samples in case of suspicions must be established and the IT service provider must take every action accordingly and ensure efficient reporting;

(f) include in the reference configuration recommended security settings which reduce the risk of malicious code infections (e.g. disable autorun or browser configuration).

There must be documented standards/procedures for providing protection against viruses, which should specify:

(g) methods for configuring virus protection software;

(h) update mechanisms and frequencies for virus protection software and a process for dealing with virus attacks;

(i) standard reference configuration for all systems, e.g. desktops, servers, laptops and handheld computing devices (e.g. PDAs).

End users must be:

(j) warned of the dangers posed by computer viruses and cyber-attacks, and trained to be aware of signs of abnormal system behaviour (e.g. slow running, new processes);

(k) notified quickly of significant new virus risks (e.g. by e-mail).

End users must:

(l) report suspected or actual virus attacks to a single point of contact for support (e.g. a help desk) and avoid attempting to remove suspected viruses themselves;

(m) keep the existing configuration of the virus protection software, and not disable or change the configuration of the virus protection software, or attempt to bypass it.

5.2.3. Checks

Regular checks must be performed to ensure that:

(a) virus protection software has not been disabled;

(b) the configuration of virus protection software is still correct;

(c) all updates have been applied effectively;

(d) emergency procedures are in place to deal with a virus incident;

(e) reports are sent to the concerned persons;

(f) the effectiveness of the virus protection is maintained: monitor the patterns of virus infections, false positives, false negatives etc. and take corrective actions responsibly.

5.2.4. Protection against malicious code at the Network Level[7]

Virus protection software at the Gateway level must be configured to:

[7] Other preventive measures specific to intrusion detection/prevention systems, network authentication or firewalls are not covered in this standard.

(a) scan and filter the incoming and outgoing network traffic (Email, HTTP, FTP and other messaging) for real-time detection and protection of malicious code[8];

5.3. Roles and Responsibilities

The Information Systems Security Policy requires the definition of security roles and responsibilities, and some of them are defined in the decision C(2006)3602. The following security roles will take part in the implementation and management of controls against malicious code:

(1) System owner

(2) IT service provider

(3) Information resource managers (IRMs)

(4) Local Informatics Security Officer (LISO)

(5) Security Directorate

(6) Users

Detailed responsibilities are defined in specific sections of this standard.

A **RACI chart** – a form of responsibility assignment matrix, linking activities to roles; responsibilities used in this standard are **R**esponsible (carries out the actual work), **A**ccountable (approves the completed work and is fully accountable for it), **C**onsulted (must be consulted beforehand - is part of two-way communication), **I**nformed (informed about progress and results - one-way communication).

[8] As a result of scanning and filtering the traffic, suspected malware generation servers must be blocked, but this is the subject of another standard;

Roles / Controls	System owners	IT service providers (e.g. DIGIT)	Information resource managers	Security Directorate	LISO	Users
Configuration	A	R	R (5.2.1 l)	C	C	
Installation and procedures	A	R	R (5.2.2 b)	C	C	R (5.2.2 l) R (5.2.2 m)
Checks	A	R	R		C	
Protection against malicious code at the Network Level	A	R		C	C	

6. REFERENCES

Commission Decision C(2006) 3602 of 16/8/2006

Implementing rules for Commission Decision C(2006) 3602 of 16.8.2006.

International standard ISO/IEC 27001 – Second edition 2005-06-15.

International standard ISO/IEC 17799 – Second edition 2005-06-15.

7. RELATED STANDARDS AND GUIDELINES

Standard on Network Security Management

Standard on Information System Security Incident Management

Standard on Information Security Risk Management